

文章编号:1671-251X(2014)11-0022-04

DOI:10.13272/j.issn.1671-251x.2014.11.006

陈运启,许金.基于元数据与角色的煤矿综合信息管理系统权限控制模型设计与实现[J].工矿自动化,2014,40(11):22-25.

基于元数据与角色的煤矿综合信息管理系统 权限控制模型设计与实现

陈运启, 许金

(中煤科工集团重庆研究院有限公司, 重庆 400039)

摘要:分析了现有煤矿信息管理系统中权限控制策略的不足,指出基本的账户控制策略不仅功能简单,且在系统运行过程中无法修改权限,而基于角色的访问控制策略缺少对系统数据的区分,不利于系统的扩展与维护;提出了基于元数据与角色的权限控制模型,通过对用户可访问元数据范围的配置与限制,实现了对用户功能权限和数据权限的管理,并通过元控件实现了权限管理的模块化设计与开发,减少了代码重复率和逻辑复杂度。该模型已应用于多个煤矿综合信息管理系统中,具有很好的灵活性和可操作性。

关键词:煤矿信息管理系统;权限管理;权限控制;基于角色的访问控制;元数据;元控件

中图分类号:TD672

文献标志码:A

网络出版时间:

网络出版地址:

Design of an access control model based on meta-data and role for
integrated information management system of coal mine and its implementation

CHEN Yunqi, XU Jin

(CCTEG Chongqing Research Institute, Chongqing 400039, China)

Abstract: Shortcomings of access control strategy in existing information management systems of coal mine were analyzed, and some views were pointed out that basic functions of account control strategy was simple in function and immutable in right during system running, and role-based access control strategy was lack of distinction of system data, which led to difficulty of system development and maintenance. An access control model based on meta-data and role was proposed, which implemented right management of user functions and data through configuring and limiting scope of accessing meta-data. Modular design and development of right management were realized by meta-control which reduced code repetition and logic complexity. The model has been used in a couple of integrated information management systems of coal mine and shows good flexibility and operability.

Key words: information management system of coal mine; right management; access control; role-based access control; meta-data; meta-control

0 引言

近年来,随着计算机及网络技术的不断发展与

应用,煤矿信息化方向逐渐从安全生产过程控制向综合信息管理平台迈进,从具有针对性且功能单一的控制子系统,向涉及多部门、多业务的综合信息管

收稿日期:2014-03-14;修回日期:2014-09-16;责任编辑:李明。

基金项目:“十二五”国家科技重大专项资助项目(2011ZX05041004)。

作者简介:陈运启(1984—),男,安徽萧县人,助理研究员,硕士,主要从事煤矿综合自动化与信息化、矿山物联网等方面的研究工作,E-mail: chen.yun.qi@qq.com。

理系统演化^[1]。煤矿企业、集团公司、省市监管部门等多部门协同管控理念的不断深入,各类生产数据的集中,系统功能的整合,用户的增加,使得煤矿信息管理系统的安全问题受到越来越多的重视和关注。权限管理是涉及信息管理系统安全的核心问题之一。一个用户可以拥有多个权限,一个权限也可以分配给多个合法用户使用。如何管理好用户与权限之间的关系,并合理控制不同级别用户访问不同范围的数据,成为煤矿综合信息管理系统开发和建设的重要研究内容。

1 现有煤矿信息管理系统权限控制策略及其不足

由于煤矿信息化建设起步较晚,权限控制策略在煤矿信息管理系统中的实现较为简单,多数安全生产过程控制系统采用基本的账户控制,极少数信息管理系统借鉴了基于角色的访问控制(Role-Based Access Control, RBAC)理论^[2]来实现系统权限管理。

1.1 基本的账户控制

煤矿安全生产过程控制系统,如水泵控制系统^[3]、通风机在线监测系统^[4]等,其功能单一,大多是对某个或某几个设备的开停进行控制、打印报表等,采用 PLC 与组态软件实现数据采集、过程控制以及生产环境的模拟。其权限控制大多通过安全区来实现,无法满足现有煤矿综合信息管理系统的要求。

较安全生产过程控制系统复杂的生产安全管理系统,如瓦斯监控系统、人员定位系统、瓦斯抽放系统等,其功能相对较多,有更进一步的权限控制要求,如设备操控、通信源码查看、特殊报表打印等功能,只有具备相应权限的人员才能进行操作。这些系统具备基本安全控制管理,在进行特殊功能操作之前需核对密码,或增加管理员账户和一般账户,其功能权限在软件编码时分配好,系统运行过程中无法进行权限分配与修改。

1.2 基于角色的访问控制

随着煤矿信息化的不断发展,煤矿生产综合管理系统及多级监管系统不断实施,涉及的数据及业务量大,不同级别的用户参与广泛,决定了这些系统必须具备较生产过程控制系统和生产安全管理系统更加严密合理的用户权限控制策略。RBAC 成为各系统实现权限控制的主要依据^[5]。

RBAC 模型经过多年的发展,衍生出很多改进模型,但其基本原理都是通过创建不同角色,将某些

不同的权限分配给相应的角色,再通过给某个用户分配其所属角色,实现用户对某些权限的操作与控制,做到用户与权限分离^[6]。这在多用户、多角色的煤矿综合信息管理系统中非常有效。

RBAC 模型包括用户、权限、角色和会话 4 个主要元素^[7],各元素之间的关系如图 1 所示。权限是指对系统中某些资源如页面、窗口、菜单等的某些操作,如添加、修改、删除、查询等。会话是由用户发起并在用户登录之后,根据系统分配的角色而获取的权限列表。

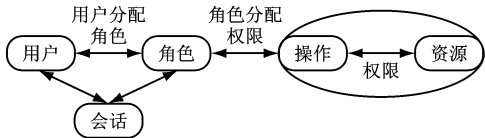


图 1 RBAC 模型 4 个元素之间的关系

煤矿综合信息管理系统涉及的用户特别多,为每位用户分别指派角色非常繁琐,因此可以结合用户组的概念,将角色指派给用户组,该组内所有用户具有该用户组的角色权限,实现角色权限批量分配和修改功能^[8]。

RBAC 模型应用于煤矿综合信息管理系统中也暴露出许多缺点,主要体现在只针对具体功能实现了权限访问控制,没有对功能涉及的数据做严格的区分,也没有对数据权限进行分类,这对涉及煤矿企业、集团公司、监管部门等不同级别的多实体、多人员参与的综合信息管理系统来讲,实用性和扩展性不强;许多对数据权限的控制都是通过直接编码的方式实现的,在系统部署后无法提供对数据权限控制的配置,为系统开发和维护带来很大难度,也无法满足用户使用过程中的变化要求。

本文在 RBAC 模型基础上,提出了元数据与角色相结合的访问控制模型,不仅实现了对某个具体功能的权限控制,而且实现了该功能下不同用户可访问数据范围的控制。

2 基于元数据与角色的访问控制模型设计

2.1 元数据与元控件

元数据是用来描述数据及其环境的数据。本文涉及的元数据主要是指构成煤矿综合信息管理系统的基础数据,如部门数据、设备类型数据、地址地点数据、用户职位级别数据等,以及其他用来描述系统数据的数据,还包括某些表示范围和阶段的数据,如时间、金额等。

由于元数据是组成系统数据的数据,可通过控

制元数据,如选择查询条件、设定数据范围等来控制用户对其他数据操作的权限限制,从而实现对系统的数据权限管理。

元控件是指展示某种元数据集合的控件,如部门下拉列表控件、查询时间范围控件等。无论在哪个功能界面或窗口中,相同元数据的表现形式和数据源固定,元控件根据当前用户可操作的元数据权限集合来显示其可操作的元数据内容,如具有不同权限的用户对部门列表进行操作时,部门列表元控件显示和可操作的数据会有所不同。假设 2 个用户的部门元数据集合分别为 User1. Metadata. DepartmentList=[胜利煤矿{职能部门<矿领导|办公室|人事部>},{采掘部门<采煤一队|采煤二队|采煤三队|掘进一队>}],User2. Metadata. DepartmentList=[胜利煤矿{职能部门<矿领导|办公室|人事部>}],则窗口或界面显示时首先执行部门元控件的初始化函数 MetaControl. DepartmentCombotree. Init (CurrentUser. Metadata. DepartmentList)。图 2 为元数据与元控件之间的关系及显示结果。

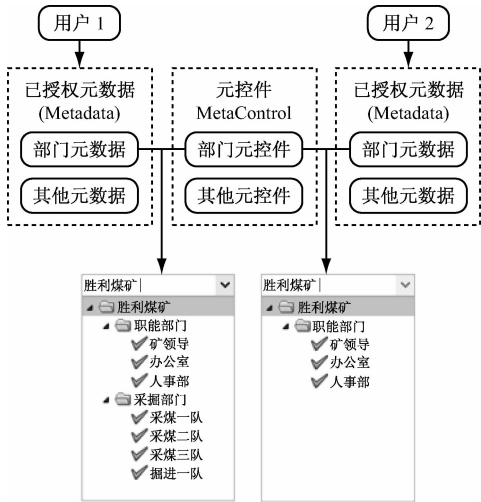


图 2 元数据与元控件之间的关系及显示结果

2.2 基于元数据与角色的访问控制模型

基于元数据与角色的访问控制模型如图 3 所示。该模型与 RBAC 模型的主要区别在于引入了元数据和元数据组。用户会话中不仅保存了用户可操作权限,还保存了用户可操作的所有元数据的范围,并在验证功能权限的基础上增加了对元数据的验证。

用户登录后,针对某个功能的权限及数据控制流程如图 4 所示。根据此次登录后会话中的用户权

限列表来判断用户是否具有该功能权限,如果没有通过权限验证,则无法完成该功能操作;如果通过权限验证,则获取该用户所具有的元数据范围,并以此来初始化当前功能页面所有的元控件,如部门列表元控件,使其只显示该用户可操作的部门列表,保证之后的相关业务处理都在该用户可操作元数据范围内进行,实现了功能权限管理及用户数据范围的验证。

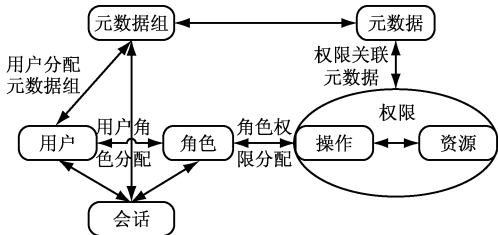


图 3 元数据与角色相结合的访问控制模型

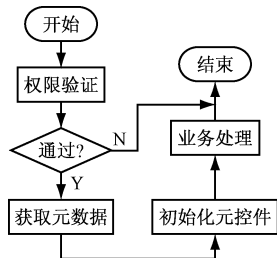


图 4 权限及数据控制流程

授权用户的元数据访问列表决定了每个元控件的元数据显示内容。该访问列表可通过配置的功能来实现,与用户角色和功能权限之间的配置一致,可根据实际需要灵活改变,无需对业务逻辑处理部分的代码做任何改动,彻底消除了将数据控制逻辑写入后台代码对业务流程更改和权限管理带来的不便。

3 基于元数据与角色的访问控制模型实现

基于元数据与角色的访问控制模型是对 RBAC 模型的扩展,而对 RBAC 模型的实现较容易,需要重点考虑如何在 C/S 与 B/S 模式下实现元控件对元数据的封装。

基于 .NET 平台的 WinForm 开发可使用自定义控件^[9]实现封装元数据的元控件。在系统开发过程中,只需将自定义元控件拖动到窗口中,每个元控件从当前应用程序用户会话缓存中读取该用户的元数据权限,即可自动实现元数据的筛选与展示,完成对数据权限的控制。

基于 ASP.NET 的 Web 系统开发可使用用户控件^[10]对元数据进行封装。采用 ASP.NET MVC

开发的系统也可使用分部视图^[11]的方式定义元控件,实现数据权限控制。

4 基于元数据与角色的访问控制模型应用优势

(1) 实现了对用户数据权限的个性化配置。与煤矿企业相关的信息化管理和监管涉及单位和部门繁杂,用户众多。通过基于元数据与角色的访问控制模型设计的煤矿综合信息管理系统元数据权限配置界面可以很方便地调整每个用户或用户组可操作的元数据及其范围。

(2) 符合模块化设计与开发的原则,减少重复。煤矿综合信息管理系统在设计与开发时,通过使用元控件可将元数据的操作进行统一封装,实现系统的模块化设计与开发,有利于编码实现和后期的更改与维护。

(3) 减少代码中的逻辑复杂度。所有对数据的权限验证与控制全部在元控件中实现,无需对外部代码进行逻辑验证。

(4) 减少数据的传输量,减轻系统负担。部分系统开发时,为了满足设计与编码的要求,将某些功能的数据由数据库服务器全部传输到应用程序中,再根据用户信息,通过逻辑分析对数据进行过滤和显示,不仅增加了数据传输量,加重网络负担,还造成一定的安全隐患,给非法用户在传输过程中拦截数据提供了条件。基于元数据与角色的访问控制模型通过对元数据的控制,只请求权限范围内的数据,避免了网络负担和安全隐患问题。

5 结语

基于元数据与角色的访问控制模型在 RBAC 模型基础上,增加了对元数据的访问限制,从而实现了完整的功能权限控制和数据访问范围控制。该模型可通过角色、权限、元数据等配置功能,很好地编

辑用户功能权限和数据权限,有利于系统维护和扩展,满足多种煤矿综合信息管理系统中权限管理的要求。该模型目前已应用于煤矿隐患管理与事故预防系统、煤矿协同控制管理系统、煤矿安全监控联网系统以及煤层气安全信息管理平台中,具有很好的灵活性和可操作性。

参考文献:

- [1] 王玮. 煤矿企业信息化建设[J]. 煤炭技术, 2010, 29(8):162-164.
- [2] SANDU R S, COYNE E J, FEINSTEIN H L, *et al.* Role-based access control models [J]. IEEE Computer, 1996, 29(2):38-47.
- [3] 槐利, 谭一川, 徐育军, 等. 煤矿井下主排水自动控制系统的应用[J]. 工矿自动化, 2012, 38(3):63-65.
- [4] 安赛, 林柏泉. 主要通风机远程监测系统的设计[J]. 工矿自动化, 2012, 38(1):4-7.
- [5] 卞宝银, 王一莉. 煤矿企业信息管理系统权限访问控制应用研究[J]. 煤炭技术, 2010, 29(4):183-185.
- [6] 黄刚, 王汝传, 田凯. 基于 RBAC 策略的可信网格访问控制模型[J]. 计算机应用研究, 2010, 27(4):1473-1476.
- [7] 信科, 杨峰, 杨光旭, 等. 基于 RBAC 权限管理系统的优化设计与实现[J]. 计算机技术与发展, 2011, 21(7):172-174.
- [8] 李龙龙, 朱高中. 通用权限管理系统的设计[J]. 科技信息, 2013(13):41-42.
- [9] 陈锋. C# 程序设计中自定义控件的创建与应用[J]. 软件导刊, 2013, 12(6):20-23.
- [10] 刘亚, 黄晓放. 基于 .NET 自定义控件的研究与设计[J]. 武汉理工大学学报:信息与管理工程版, 2009, 31(6):873-876.
- [11] 方柯. 基于 ASP.NET MVC 框架的 Web 应用开发研究[D]. 上海:华东师范大学, 2011.